Computing functions on Jacobians and their quotients

Jean-Marc Couveignes, Tony Ezome

COMPUTING FUNCTIONS ON JACOBIANS AND THEIR QUOTIENTS

JEAN-MARC COUVEIGNES AND TONY EZOME

ABSTRACT. We show how to efficiently evaluate functions on jacobian varieties and their quotients. We deduce a quasi-optimal algorithm to compute (l, l) isogenies between Jacobians of genus two curves.

CONTENTS

1. INTRODUCTION

We consider the problem of computing the quotient of the jacobian variety J_C of a curve C by a maximal isotropic subgroup V in its l-torsion for l an odd prime integer. The genus one case has been explorated a lot since Vélu [27, 28]. A recent bibliography can be found in [3].

Date: November 1, 2014.

In this work we first study this problem in general, showing how to quickly design and evaluate functions on the quotient J_C/V. We then turn to the specific case when the dimension g of J_C equals two. In that case, the quotient is, at least generically, the Jacobian of another curve D. The quotient isogeny can then be described in a compact form: a few rational fractions of degree $O(l)$. We explain how to compute D and the embedding of C in the Jacobian of D in quasi-linear time in $\#V = l^2$.

Plan In Section 2 we bound the complexity of evaluating standard functions on Jacobians, including Weil functions and algebraic Theta functions. We deduce in Section 3 a bound for the complexity of computing a basis of sections for the bundle associated with a multiple of the natural polarization of J_C. We recall the algebraic definition of canonical Theta functions in Section 4 and bound the complexity of evaluating such a function at a given point in J_C. Section 5 bounds the complexity of evaluating functions on the quotient of J_C by a maximal isotropic subgroup V in $J_C[l]$ when l is an odd prime different from the characteristic of $\mathbf{K}$. Specific algorithms for genus two curves are given in Section 6. A complete example is treated in Section 7.

Context The algorithmic aspect of isogenies was explorated by Vélu [27, 28] in the context of elliptic curves. He exhibits bases of linear spaces made of Weil functions, then finds invariant functions using traces. Vélu considers the problem of computing the quotient variety once given some finite subgroup. The problem of computing (subgroups of) torsion points is independent and was solved in a somewhat optimal way by Elkies [10] in the genus one case, using modular equations. It is unlikely that modular equations will be of any use to accelerate the computation of torsion points for higher genera, since they all are far too big. Torsion points may be computed by brute force (torsion polynomials), using the Zeta function when it is known [6], or because they come naturally as part of the input (modular curves). We shall not consider this problem and will concentrate on the computation of the isogeny, once given its kernel. The genus one case has been surveyed by Schoof [24] and Lercier-Morain [16]. The genus two case was studied by Dolgachev and Lehavi [9], and Smith [26], who provide a very elegant geometric description. However the complexity of the resulting algorithm is not given (and is not optimal anyway). Lubicz and Robert [17, 18] provide general methods for quotienting abelian varieties (not necessarily Jacobians) by maximum isotropic subgroups in the l-torsion. Their method has quasi-optimal complexity $l^{g(1+o(1))}$ when l is a sum of two squares. Otherwise it has complexity $l^{g(2+o(1))}$. The case of dimension two is treated by Cosset and Robert [5]. They reach complexity $l^{2+o(1)}$ when l is the sum of two squares and $l^{4+o(1)}$ otherwise. However, the input and mainly the output of these methods is quite different from ours. In the dimension two case, we can, and must provide a curve D of which J_C/V is the Jacobian, and an explicit map from C into the symmetric square of D. We achieve this goal in quasi-optimal time $l^{2+o(1)}$ for every odd prime $l \neq p$.

Notation Let $\mathbf{K}$ be a field, $\bar{\mathbf{K}}$ an algebraic closure of $\mathbf{K}$, and C a projective, smooth, absolutely integral curve over $\mathbf{K}$. Let g be the genus of C. We assume that $g \geq 2$ and we call J_C the Jacobian of C. The linear equivalence class of a divisor D is denoted D also if there is no risk of confusion. The canonical class is denoted $K_C \in \mathrm{Pic}^{2g-2}(C)$. We call $\mathrm{W} \subset \mathrm{Pic}^{g-1}(C)$ the algebraic set of classes of effective divisors of degree $g-1$. The pullback $[-1]^*\mathrm{W} \subset \mathrm{Pic}^{1-g}(C)$ is equal to the translate $\mathrm{W} - K_C$ of W by $-K_C$. If there exists a $\mathbf{K}$-rational point Θ in $\mathrm{Pic}^{g-1}(C)$ such that 2Θ

is the canonical class, then we translate W into J_C by subtracting Θ to every class in it. The resulting divisor is denoted $\mathcal{W} = \mathrm{W} - \Theta$. One has

$$[-1]^*\mathcal{W} = \mathcal{W}.$$

Such a Θ is called a *Theta characteristic*. Given a $\mathbf{K}$-rational point O on C, we translate W into J_C by subtracting $(g-1)O$ to every class in it. The resulting algebraic subset of J_C is denoted $W = \mathrm{W} - (g-1)O$. We call $\kappa \in J_C$ the class of $K_C - 2(g-1)O$. For every u in J_C we call

$$t_u : J_C \to J_C$$

the translation by u and $W_u = t_u(W) = W + u$ the translation of W by u. We have

$$[-1]^*W = W_{-\kappa}.$$

We let ϑ be the class of $\Theta - (g-1)O$ in J_C and we check that

$$\mathcal{W} = W_{-\vartheta}.$$

Given D a divisor on C we write $\mathcal{L}(D)$ for the linear space $H^0(C, \mathcal{O}_C(D))$ and $\ell(D)$ for its dimension.

Aknowledgements We thank Damien Robert for his comments on an early version of this work and Qinq Liu for interesting discussions about holomorphic differentials. This research is supported by the “Agence Nationale de la Recherche” (project PEACE) and by the cluster of excellence CPU (Numerical certification and reliability).

2. Functions on Jacobians

Constructing functions on abelian varieties using zero-cycles and divisors is classical [30, 31]. In this section, we bound the complexity of evaluating such functions in the special case of jacobian varieties. Let $\mathfrak{u} = \sum_{1\le i\le I} e_i[u_i]$ be a zero-cycle in J_C, where $(e_1, e_2, \dots, e_I) \in \mathbf{Z}^I$ and $(u_1, \dots, u_I) \in J_C^I$. Set

$$s(\mathfrak{u}) = \sum_{1\le i\le I} e_i u_i \in J_C \text{ and } \deg(\mathfrak{u}) = \sum_{1\le i\le I} e_i \in \mathbf{Z}.$$

The divisor $\sum_{1\le i\le I} e_i W_{u_i} - W_{s(\mathfrak{u})} - (\deg(\mathfrak{u}) - 1)W$ is principal. Let y be a point on J_C not in the support of this divisor. Call $\eta_W[\mathfrak{u}, y]$ the unique function on J_C having divisor

$$(\eta_W[\mathfrak{u}, y]) = \sum_{1\le i\le I} e_i W_{u_i} - W_{s(\mathfrak{u})} - (\deg(\mathfrak{u}) - 1)W$$

and such that

$$\eta_W[\mathfrak{u}, y](y) = 1.$$

This definition is additive in the sense that

$$\eta_W[\mathfrak{u} + \mathfrak{v}, y] = \eta_W[\mathfrak{u}, y] \times \eta_W[\mathfrak{v}, y] \times \eta_W[[s(\mathfrak{u})] + [s(\mathfrak{v})], y] \tag{1}$$

whenever it makes sense, and in particular for y a generic point on J_C. This relation allows us to evaluate Eta functions by pieces: we first treat a few special cases and then explain how to combine them to efficiently evaluate any Eta function. We write $\eta_W[\mathfrak{u}] \in \mathbf{K}(J_C)^*/\mathbf{K}^*$ when we consider an Eta function up to a multiplicative scalar.

2.1. **An easy special case.** To every non-zero function f on C one can naturally [7] associate a function $\alpha[f]$ on J_C in the following way. We assume that f has degree d and divisor

$$(f) = \sum_{1\le i\le d} Z_i - \sum_{1\le i\le d} P_i.$$

Let x be a point on J_C such that $x \notin W_{P_i}$ for every $1 \le i \le d$. In particular $\ell(x + gO) = 1$. Let D_x be the unique effective divisor of degree g such that $D_x - gO$ belongs to the class x. Write $D_x = D_1 + D_2 + \cdots + D_g$ and set

$$\alpha[f](x) = f(D_1) \times f(D_2) \times \cdots \times f(D_g). \tag{2}$$

The divisor of $\alpha[f]$ is

$$(\alpha[f]) = \sum_{1\le i\le d} W_{Z_i} - \sum_{1\le i\le d} W_{P_i}$$

where the Z_i and the P_i are seen as points in J_C via the Jacobi integration map with origin O. Let y be a point in J_C such that $y \notin W_{P_i}$ and $y \notin W_{Z_i}$ for every $1 \le i \le d$. Then

$$\alpha[f](x)/\alpha[f](y) = \eta_W[\sum_{1\le i\le d}[Z_i] - \sum_{1\le i\le d}[P_i], y](x).$$

2.2. **Algorithmic considerations.** Having described in Section 2.1 a first method to evaluate Eta functions in some special case, we bound the complexity of this method. We take this opportunity to set some notation and convention.

2.2.1. *Notation.* In this text, the notation $\mathfrak{O}$ stands for a positive absolute constant. Any statement containing this symbol becomes true if the symbol is replaced in every occurrence by some large enough real number. Similarly, the notation $\mathfrak{e}(x)$ stands for a real function of the real parameter x alone, belonging to the class $o(1)$.

2.2.2. *Operations in* $\mathbf{K}$. The time needed for one operation in $\mathbf{K}$ is a convenient unit of time. Let $\mathbf{L}$ be a monogene finite $\mathbf{K}$-algebra of degree d. We will assume that $\mathbf{L}$ is given as a quotient $\mathbf{K}[x]/f(x)$ where $f(x)$ is a polynomial in $\mathbf{K}[x]$. Every operation in $\mathbf{L}$ requires $d^{1+\mathfrak{e}(d)}$ operations in $\mathbf{K}$. When $\mathbf{K}$ is a finite field with cardinality q, every operation in $\mathbf{K}$ requires $(\log q)^{1+\mathfrak{e}(q)}$ elementary operations.

2.2.3. *Operations in* $J_C(\mathbf{K})$. Elements in $J_C(\mathbf{K})$ are classically represented by divisors on C. We can also use Makdisi's representation [14] which is more efficient. For our purpose it will be enough to know that one operation in $J_C(\mathbf{K})$ requires $g^{\mathfrak{O}}$ operations in $\mathbf{K}$ that is $g^{\mathfrak{O}} \times (\log q)^{1+\mathfrak{e}(q)}$ elementary operations when $\mathbf{K}$ is a field with q elements. Given two effective divisors D and E with respective degrees d and e, we are able to compute a basis of $\mathcal{L}(D - E)$ at the expense of $(gde)^{\mathfrak{O}}$ operations in $\mathbf{K}$. Possible references for these classical algorithms are Diem [8], Volcheck [29], Poonen [23], or the quick account at the beginning of [6].

2.2.4. *Evaluating* $\alpha[f]$. We are given a function f on C. We are given a class x in J_C, represented by $D_x - gO$ where D_x is effective with degree g. We may see D_x as a zero-dimensional scheme over $\mathbf{K}$, and call $\mathbf{K}[D_x]$ the associated affine $\mathbf{K}$-algebra. We assume that D_x does not meet the poles of f. Let P be the generic point on D_x. Then $f(P)$ belongs to $\mathbf{K}[D_x]$ and its norm over $\mathbf{K}$ is $\alpha[f](x)$ according to the definition given in Equation (2). Thus we can compute $\alpha[f](x)$ at the expense of $(gd)^{\mathfrak{O}}$ operations in $\mathbf{K}$, where g is the genus of C and d is the degree of f.

2.3. **Determinants.** The evaluation method presented in Section 2.2 only applies to Alpha functions introduced in Section 2.1. These Alpha functions form a subfamily of Eta functions. Mascot [19] introduced an efficient evaluation method that applies to another interesting subfamily.

One can also define and evaluate [1, 11, 25] functions on J_C using determinants. We shall see that every Eta function can be expressed as a combination of Alpha functions, as in Section 2.1, and determinants. Let D be a divisor on C with degree $d \geq 2g-1$. Set

$$n = \ell(D) = d - g + 1.$$

Let $f = (f_k)_{1\leq k\leq n}$ be a basis of $\mathcal{L}(D)$. For $P = (P_l)_{1\leq l\leq n}$ in C^n disjoint from the positive part of D we set

$$\beta[f](P) = \det(f_k(P_l))_{k,l}$$

and thus define a function $\beta[f]$ on C^n. We call $j^n : C^n \to \mathrm{Pic}^n(C)$ the Jacobi integration map. We call $\pi_l : C^n \to C$ the projection onto the l-th factor. We call $\Delta \subset C^n$ the full diagonal. The divisor of $\beta[f]$ is

$$(\beta[f]) = \Delta + (j^n)^*([-1]^*\mathrm{W} + D) + \sum_{1\leq l\leq n} \pi_l^*(-D)$$

where $[-1]^*\mathrm{W} + D = \mathrm{W} - K_C + D \subset \mathrm{Pic}^n(C)$ is the translate of $[-1]^*\mathrm{W}$ by the class of D.

We now assume that we have a collection of divisors $D = (D^{(i)})_{1\leq i\leq I}$. We assume that all $D^{(i)}$ have degree $d = 2g-1$. So $n = \ell(D^{(i)}) = g$. We are given a vector of integers $e = (e_i)_{1\leq i\leq I}$ such that $\sum_{1\leq i\leq I} e_i = 0$. For every i we choose a basis $f^{(i)} = (f_k^{(i)})_{1\leq k\leq g}$ of $\mathcal{L}(D^{(i)})$. We assume that $\sum_{1\leq i\leq I} e_i \times D^{(i)}$ is the (principal) divisor of some function h on C. We call $\alpha[h]$ the function on J_C associated with h, as constructed in Section 2.1. We set $f = (f^{(i)})_{1\leq i\leq I}$. Define the function

$$\beta[D, e, f] = \prod_{1\leq i\leq I} \beta[f^{(i)}]^{e_i}$$

on C^g. It has divisor

$$(\beta[D, e, f]) = \sum_i e_i \times (j^g)^*(\mathrm{W} + D^{(i)} - K_C) - \sum_{\substack{1\leq i\leq I \\ 1\leq l\leq g}} e_i \times \pi_l^*(D^{(i)}).$$

There exists a function $\beta'[D,e,f]$ on $\mathrm{Pic}^g(C)$ such that $\beta[D,e,f] = \beta'[D,e,f] \circ j^n$. Indeed, permuting the g points $(P_i)_{1\leq i\leq g}$ multiplies each factor $\beta[f^{(i)}]$ by the same sign. We call $\gamma[D,e,f]$ the function on $J_C = \mathrm{Pic}^0(C)$ obtained by composing $\beta'[D,e,f]$ with the translation by gO. The product $\gamma[D,e,f] \times \alpha[h]$ has divisor

$$(\gamma[D,e,f]) + (\alpha[h]) = \sum_i e_i W_{u_i},$$

where

$$u_i = D^{(i)} - K_C - O \in J_C.$$

We deduce that $\gamma[D, e, f] \times \alpha[h]$ is equal to $\eta_W[\mathfrak{u}]$ in $\mathbf{K}(J_C)^*/\mathbf{K}^*$ where $\mathfrak{u} = \sum_i e_i[u_i]$.

2.4. **Evaluating Eta functions.** We explain how to evaluate Eta functions, using the product decomposition given in Section 2.3. We are given $\mathfrak{u} = \sum_{1\le i\le I} e_i[u_i]$ a zero-cycle in J_C. We can and will assume without loss of generality that $\deg(\mathfrak{u}) = \sum_i e_i = 0$ and $s(\mathfrak{u}) = \sum_i e_i u_i = 0$. We are given two classes x and y in $J_C(\mathbf{K})$. The class x is represented by a divisor $D_x - gO$ where D_x is effective with degree g. The class y is represented similarly by a divisor $D_y - gO$. We assume that y does not belong to the support of the divisor $\sum_{1\le i\le I} e_i W_{u_i}$. We want to evaluate $\eta_W[\mathfrak{u}, y](x)$.

The algorithm goes as follows.

(1) For every $1 \le i \le I$, find an effective divisor $D^{(i)}$ of degree $2g - 1$ such that $D^{(i)}$ does no meet D_x nor D_y, and $D^{(i)} - K_C - O$ belongs to the class u_i.
(2) Find a non-zero function h in $\mathbf{K}(C)$ with divisor $\sum_{1\le i\le I} e_i D^{(i)}$.
(3) For every $1 \le i \le I$, compute a basis $f^{(i)} = (f_k^{(i)})_{1\le k\le g}$ of $\mathcal{L}(D^{(i)})$.
(4) Write $D_x = X_1 + X_2 + \cdots + X_g$ and $D_y = Y_1 + Y_2 + \cdots + Y_g$ where X_k and Y_k are points in $C(\bar{\mathbf{K}})$ for $1 \le k \le g$. For every $1 \le i \le I$, compute
$$\delta_x^{(i)} = \det(f_k^{(i)}(X_l))_{1\le k,l\le g} \text{ and } \delta_y^{(i)} = \det(f_k^{(i)}(Y_l))_{1\le k,l\le g}.$$
(5) Compute $\alpha[h](x)$ and $\alpha[h](y)$.
(6) Return
$$\frac{\alpha[h](x)}{\alpha[h](y)} \times \prod_{1\le i\le I} (\delta_x^{(i)}/\delta_y^{(i)})^{e_i}.$$

We now precise every step. In step (1) we assume that the class u_i is given by a divisor $U_i - gO$ where U_i is effective with degree g. We proceed as in [6, Lemmata 13.1.7-8-9]. We compute $\mathcal{L}(U_i - (g-1)O + K_C)$. To every non-zero function f in this linear space is associated a candidate divisor $(f) + U_i - (g-1)O + K_C$ for $D^{(i)}$. We eliminate the candidates that meet either D_x or D_y. The corresponding functions f belong to a union of at most $2g$ strict subspaces of $\mathcal{L}(U_i - (g-1)O + K_C)$. If the cardinality of $\mathbf{K}$ is bigger than $2g$ we find a decent divisor $D^{(i)}$ by solving inequalities. If $\mathbf{K}$ is too small, we can replace $\mathbf{K}$ by a small extension of it. In any case, we find some $D^{(i)}$ at the expense of $g^{\mathfrak{O}}$ operations in $\mathbf{K}$.

Step (2) is effective Riemann-Roch. It requires $(g \times |e|)^{\mathfrak{O}}$ operations in the base field, where
$$|e| = \sum_{1\le i\le I} |e_i|$$
is the ℓ^1-norm. Step (3) is similar to step (2) and requires $I \times g^{\mathfrak{O}}$ operations in $\mathbf{K}$. Step (4) requires some care. Brute force calculation with the X_k and Y_k may not be polynomial time in the genus because the degree over $\mathbf{K}$ of the decomposition field of D_x and D_y may be very large. However, if D_x is irreducible over $\mathbf{K}$, then this decomposition field has degree g, which is fine with us. In general, we write $D_x = \sum_{1\le l\le L} a_l R_l$ where the R_l are pairwise distinct irreducible divisors and the a_l are positive integers. We compute a new basis $(\phi_k)_{1\le k\le g}$ for $\mathcal{L}(D^{(i)})$ which is adapted to the decomposition of D_x in the following sense: we start with a basis of $\mathcal{L}(D^{(i)} - \sum_{l\ge 2} a_l R_l)$,

we continue with a basis of $\mathcal{L}(D^{(i)} - \sum_{l\geq 3} a_l R_l)/\mathcal{L}(D^{(i)} - \sum_{l\geq 2} a_l R_l)$, we continue with a basis of $\mathcal{L}(D^{(i)} - \sum_{l\geq 4} a_l R_l)/\mathcal{L}(D^{(i)} - \sum_{l\geq 3} a_l R_l)$, and so on. The matrix $(\phi_k^{(i)}(X_l))_{1\leq k,l\leq g}$ is block-triangular, so its determinant is a product of L determinants (one for each R_l). We compute each of these L determinants by brute force and multiply them together. We multiply the resulting product by the determinant of the transition matrix between the two bases.

For step (5) we use the method described in Section 2.2.4. Step (6) seems trivial, but it hides an ultimate difficulty. If D_x is not simple, then all $\delta_x^{(i)}$ are zero and there appear artificial indeterminacies in the product $\prod_i (\delta_x^{(i)})^{e_i}$. We use a deformation to circumvent this difficulty. We introduce a formal parameter t and consider the field $\mathbf{L} = \mathbf{K}((t))$ of formal series in t with coefficients in $\mathbf{K}$. Consider for example the worst case in which D_x is g times a point A. We fix a local parameter $z_A \in \mathbf{K}(C)$ at A. We fix g pairwise distinct scalars $(a_m)_{1\leq m\leq g}$ in $\mathbf{K}$. In case the cardinality of $\mathbf{K}$ is $< g$, we replace $\mathbf{K}$ by a small degree extension of it. We denote $X_1(t)$, $X_2(t)$, $\dots$, $X_g(t)$, the g points in $C(\mathbf{L})$ associated with the values $a_1 t$, $\dots$, $a_g t$, of the local parameter z_A. We perfom the calculations described above with D_x replaced by $D_x(t) = X_1(t) + \cdots + X_g(t)$, and set $t = 0$ in the result. Since we use a field of series, we care about the necessary t-adic accuracy. This is the maximum t-adic valuation of the $\beta[f^{(i)}](D_x(t))$. Assuming that x does not belong to the support of the divisor $(\eta_W[\mathfrak{u}]) = \sum_{1\leq i\leq I} e_i W_{u_i}$, these valuations all are equal to $g(g-1)/2$. So the complexity remains polynomial in the genus g. In case $\mathbf{K}$ is a finite field we obtain the theorem below.

Theorem 1 (Evaluating Eta functions on the Jacobian)**.** *There exists a deterministic algorithm that on input a finite field $\mathbf{K}$ with cardinality q, a curve C of genus $g \geq 2$ over $\mathbf{K}$, a zero-cycle $\mathfrak{u} = \sum_{1\leq i\leq I} e_i [u_i]$ on the jacobian variety J_C of C, and two points $x, y \in J_C$, not in $\cup_{1\leq i\leq I} W_{u_i}$, computes $\eta_W[\mathfrak{u}, y](x)$ in time $(g \times |e|)^{\mathfrak{O}} \times (\log q)^{1+\mathfrak{e}(q)}$, where $|e| = \sum_{1\leq i\leq I} |e_i|$ is the ℓ^1-norm of e.*

Remark 1. *Using fast exponentiation and Equation (1) in the algorithm above, we obtain an algorithm that evaluates Eta functions in time $g^{\mathfrak{O}} \times I \times \log|e| \times (\log q)^{1+\mathfrak{e}(q)}$. However this algorithm may fail when the argument x belongs to the support of the divisor of some intermediate factor. According to Lemma 2 below, the proportion of such x in $J_C(\mathbf{K})$ is $\leq g^{\mathfrak{O}g} \times I \times \log(|e|)/q$. Fast exponentiation for evaluating Weil functions on abelian varieties first appears in work by Miller* [20] *in the context of pairing computation on elliptic curves.*

3. Bases of linear spaces

Beeing able to evaluate Eta functions $\eta_W[\mathfrak{u}, y]$ we find a basis for $H^0(J_C, \mathcal{O}_{J_C}(lW))$. It suffices to pick random functions in this linear space. In order to justify this approach, at least when the base field is finite, we use rough consequences of Weil bounds. We recall these estimates in Section 3.1. We explain in Section 3.2 how to pick random functions in $H^0(J_C, \mathcal{O}_{J_C}(lW))$ with close enough to uniform probability.

3.1. **Number of points on Theta divisors.**

We recall a rought but very general and convenient upper bound for the number of points in algebraic sets over finite fields. It is due [12, Proposition 12.1] to Lachaud and Ghorpade.

Lemma 1 (Rough bound for the number of points)**.** *Let $\mathbf{K}$ be a field with q elements. Let X be a projective algebraic set over $\mathbf{K}$. Let n be the maximum of the dimensions of the $\mathbf{K}$-irreducible components of X. Let d be the sum of the degrees of the $\mathbf{K}$-irreducible components of X. Then*

$$|X(\mathbf{K})| \leq d(q^n + q^{n-1} + \cdots + q + 1).$$

Let $\mathbf{K}$ be a finite field with cardinality q and C a curve over $\mathbf{K}$ and O a $\mathbf{K}$-rational point on C and J_C the Jacobian of C. Let W be the algebraic susbet of J_C consisting of all classes $A - (g-1)O$ where A is an effective divisor with degree $g-1$. Let D be an algebraic set of codimention one in J_C. We assume that D is algebraically equivalent to kW. Set $l = \max(3, k)$. The divisor $E = D + (l-k)W$ is algebraically equivalent to lW. After base change to $\bar{\mathbf{K}}$ it becomes linearly equivalent to a translate of lW. Since every translate of W is ample [22, Chapter II, §6] and $l \geq 3$ we deduce [22, Chapter III, §17] that E is very ample. We now apply Lemma 1 to the hyperplane section E. Its dimension is $n = g-1$ and its degree d is $E^g = l^g W^g = l^g \times g!$ so $|D(\mathbf{K})| \leq |E(\mathbf{K})| \leq l^g \times g! \times (q^{g-1} + q^{g-2} + \cdots + q + 1) \leq g \times g! \times l^g \times q^{g-1}$. On the other hand [15, Théorème 2] the cardinality of $J_C(\mathbf{K})$ is at least $q^{g-1}(q-1)^2(q+1)^{-1}(g+1)^{-1}$. So the proportion $D(\mathbf{K})/J_C(\mathbf{K})$ is $\leq g^{\mathfrak{O}g} l^g/q$.

Lemma 2 (Number of points in hyperplane sections)**.** *Let $\mathbf{K}$ be a finite field, J_C a Jacobian of dimension $g \geq 1$ over $\mathbf{K}$, and $D \subset J_C$ an algebraic subset of codimension one, algebraically equivalent to kW for $k \geq 1$. Set $l = \max(3, k)$. The number of $\mathbf{K}$-rational points on D is bounded from above by $g \times g! \times l^g \times q^{g-1}$. The ratio $|D(\mathbf{K})|/|J_C(\mathbf{K})|$ is bounded from above by $g^{\mathfrak{O}g} l^g/q$.*

3.2. **Random Weil functions.** Fix two positive integers a and b such that $a + b = l$. For every u and y in J_C such that $y \notin W \cup W_{au} \cup W_{-bu}$ call $\tau[u, y]$ the unique function with divisor

$$(\tau[u, y]) = bW_{au} + aW_{-bu} - lW$$

such that $\tau[u, y](y) = 1$. So

$$\tau[u, y] = \eta_W[b[au] + a[-bu], y].$$

Let $\tau[u]$ be the class of $\tau[u, y]$ in $\mathbf{K}(J_C)^*/\mathbf{K}^*$. The collection of all $\tau[u]$ when u runs over the set $J_C[l](\bar{\mathbf{K}})$ is a generating set for $\mathbf{P}(H^0(J_C, \mathcal{O}_{J_C}(lW)))$. So the map $u \mapsto \tau[u]$ from J_C to $\mathbf{P}(H^0(J_C, \mathcal{O}_{J_C}(lW)))$ is non-degenerate. Hyperplane sections for this map are algebraically equivalent to $ablW$.

We pick a random element u in $J_C(\mathbf{K})$, using the Monte Carlo probabilistic algorithm given in [6, Lemma 13.2.4]. This algorithm returns a random element u with uniform probability inside a subgroup of $J_C(\mathbf{K})$ with index $\iota \leq \mathfrak{O}g^{\mathfrak{O}}$. We then consider the function $\tau[u, y]$ where y is any point in $J_C(\mathbf{K})$ not in $W \cup W_{au} \cup W_{-bu}$. According to Lemma 2, for every hyperplane H in $\mathbf{P}(H^0(J_C, \mathcal{O}_{J_C}(lW)))$, the proportion of $u \in J_C(\mathbf{K})$ such that $\tau[u]$ belongs to H is $\leq (lg)^{\mathfrak{O}g}/q$. We assume that q is large enough to make this proportion smaller than $\leq 1/(2\iota)$. The probability that $\tau[u]$ belongs to H is then $\leq 1/2$.

Proposition 1 (Random Weil functions)**.** *There exists a constant $\mathfrak{O}$ such that the following is true. There exists a probabilisitic Las Vegas algorithm that takes as input three integers $l \geq 2$, $a \geq 1$, and $b \geq 1$, such that $a + b = l$, a curve C of genus $g \geq 1$ over a field $\mathbf{K}$ with q elements, such that $q \geq (lg)^{\mathfrak{O}g}$, and returns a pair (u, y) in $J_C(\mathbf{K})^2$ such that $\eta_W[u, y]$ is a random function in*

$H^0(J_C, \mathcal{O}_{J_C}(lW))$ with probability measure μ such that $\mu(H) \le 1/2$ for every hyperplane H in $H^0(J_C, \mathcal{O}_{J_C}(lW))$. The algorithm runs in time $\mathfrak{O} \times g^{\mathfrak{O}} \times (\log l) \times (\log q)^{1+\epsilon(q)}$.

In order to find a basis of $H^0(J_C, \mathcal{O}_{J_C}(lW))$ we take $I \ge \mathfrak{O} \times l^g \times \log(l^g)$ and pick I random elements $(u_i)_{1\le i\le I}$ in $J_C(\mathbf{K})$ as explained above. For every i we find a y_i in $J_C(\mathbf{K})$ such that $y_i \notin W \cup W_{au_i} \cup W_{-bu_i}$. We pick another I elements $(w_j)_{1\le j\le I}$ such that $w_j \notin W$. We compute $\tau[u_i, y_i](w_j)$ for every pair (i, j). We put the corresponding $I \times I$ matrix in echelon form. If the rank is l^g we deduce a basis for both $H^0(J_C, \mathcal{O}_{J_C}(lW))$ and its dual all at a time.

Proposition 2 (Basis of $H^0(J_C, \mathcal{O}_{J_C}(lW))$)**.** *There exists a constant $\mathfrak{O}$ such that the following is true. There exists a probabilisitic Las Vegas algorithm that takes as input three integers $l \ge 2$, $a \ge 1$, and $b \ge 1$, such that $a + b = l$, a curve C of genus $g \ge 1$ over a field $\mathbf{K}$ with q elements, such that $q \ge (lg)^{\mathfrak{O}g}$, and returns l^g triples $(u_i, y_i, w_i) \in J_C(\mathbf{K})$ such that $(\tau[u_i, y_i])_{1\le i\le l^g}$ is a basis of $H^0(J_C, \mathcal{O}_{J_C}(lW))$ and $(w_i)_{1\le i\le l^g}$ is a basis of its dual. The algorithm runs in time $\mathfrak{O} \times g^{\mathfrak{O}} \times (l^g)^{\omega(1+\epsilon(l^g))} \times (\log q)^{1+\epsilon(q)}$ where $\omega \le 2.4$ is the exponent in matrix multiplication.*

If the condition $q \ge (lg)^{\mathfrak{O}g}$ is not met, we work with a small extension $\mathbf{L}$ of $\mathbf{K}$, then make a descent from $\mathbf{L}$ to $\mathbf{K}$ on the result. The resulting basis will consist of traces of Tau functions.

4. Canonical Theta functions

Let $l \ge 3$ be an odd prime. We assume that l is different from the characteristic p of $\mathbf{K}$. Let $L = \mathcal{O}_{J_C}(l\mathcal{W})$ be the line bundle associated to the divisor $l\mathcal{W}$. The Theta group $\mathcal{G}(L)$ fits in the exact sequence

$$1 \to \mathbf{G}_m \to \mathcal{G}(L) \to J_C[l] \to 0.$$

In this section we recall the definition of algebraic Theta functions. Restriction to the case when l is odd allows us to be slightly more effective than [21]. We bound the complexity of evaluating these Theta functions. Theta functions are useful to define descent data. We shall need them in Section 5.

4.1. **Canonical Theta functions.**

We recall the properties of canonical Theta functions as defined e.g. in [2, 3.2] or [21, §3]. We shall see that canonical Theta functions can be characterized more easily when the level l is odd. For u in $J_C[l]$ we let θ_u be a function on J_C with divisor $l(\mathcal{W}_u - \mathcal{W})$. We call

$$\mathbf{a}_u : H^0(J_C, \mathcal{O}_{J_C}(l\mathcal{W})) \to H^0(J_C, \mathcal{O}_{J_C}(l\mathcal{W}))$$

the endomorphism that maps every function f onto $\theta_u \times f \circ t_{-u}$. For the moment θ_u and $\mathbf{a}_u$ are only defined up to a multiplicative scalar. We now normalize both of them. We want the l-th iterate of $\mathbf{a}_u$ to be the identity. So $\theta_u \times \theta_u \circ t_u \times \cdots \times \theta_u \circ t_{(l-1)u}$ should be one. We therefore divide θ_u by one of the l-th roots of the above product to ensure that $\mathbf{a}_u$ has order dividing l. Now θ_u and $\mathbf{a}_u$ are defined up to an l-th root of unity. We compare $[-1] \circ \mathbf{a}_u \circ [-1]$ and $\mathbf{a}_u^{-1}$. They differ by an l-th root of unity ζ. Since l is odd, ζ has square root $\zeta^{(l+1)/2}$. Dividing $\mathbf{a}_u$ and θ_u by this square root we complete their definition.

Proposition 3 (Canonical Theta functions)**.** *For every u in $J_C[l]$ there is a unique function θ_u with divisor $l(\mathcal{W}_u - \mathcal{W})$ such that*

$$\theta_u \times \theta_u \circ t_u \times \cdots \times \theta_u \circ t_{(l-1)u} = 1 \tag{3}$$

and

$$\theta_u \circ [-1] = (\theta_u \circ t_u)^{-1}. \tag{4}$$

Further $\theta_{-u} = \theta_u \circ [-1]$. The map $u \mapsto \theta_u$ is Galois equivariant: for every σ in the absolute Galois group of $\mathbf{K}$ we have

$${}^{\sigma}\theta_u = \theta_{\sigma(u)}.$$

Let $\mathbf{a}_u$ be the endomorphism

$$\begin{array}{rccc} \mathbf{a}_u : & H^0(J_C, \mathcal{O}_{J_C}(l\mathcal{W})) & \longrightarrow & H^0(J_C, \mathcal{O}_{J_C}(l\mathcal{W})) \\ & & & \\ & f & \longmapsto & \theta_u \times f \circ t_{-u}. \end{array}$$

we have $\mathbf{a}_u^l = 1$ and $[-1] \circ \mathbf{a}_u \circ [-1] = \mathbf{a}_{-u} = \mathbf{a}_u^{-1}$. The map $u \mapsto \mathbf{a}_u$ is Galois equivariant.

Proof. There only remains to prove the equivariance property. It follows from the equivariance of conditions (3) and (4). □

For u and v in $J_C[l]$ we write

$$e_l(u,v) = \mathbf{a}_u \mathbf{a}_v \mathbf{a}_u^{-1} \mathbf{a}_v^{-1} \in \mu_l$$

for the commutator pairing and

$$f_l(u,v) = \sqrt{e_l(u,v)} = (e_l(u,v))^{\frac{l+1}{2}}$$

for the half pairing. We check that

$$\theta_{u+v} = f_l(u,v)\theta_v \times \theta_u \circ t_{-v} = f_l(v,u)\theta_u \times \theta_v \circ t_{-u}, \tag{5}$$

and

$$\mathbf{a}_{u+v} = f_l(u,v)\mathbf{a}_v \mathbf{a}_u = f_l(v,u)\mathbf{a}_u \mathbf{a}_v,$$

and

$$\mathbf{a}_u(\theta[v]) = f_l(u,v)\theta[u+v].$$

4.2. **Evaluating canonical Theta functions.** We relate the canonical Theta functions to the Eta functions introduced in Section 2 and show how to evaluate them. We assume that we are given u and x in $J_C(\mathbf{K})$ with $lu = 0$, and we want to evaluate $\theta_u(x)$. We assume that $x \notin \mathcal{W}$. Since l is odd we set

$$v = \frac{l+1}{2} \times u \in J_C(\mathbf{K}).$$

We deduce from Equation (5) that

$$\theta_u(x) = \theta_v(x) \times \theta_v(x - v)$$

provided that $x \notin \mathcal{W}_v$. On the other hand we deduce from Equation (4) that

$$\theta_v(x) \times \theta_v(v - x) = 1$$

provided that $x \notin \mathcal{W} \cup \mathcal{W}_v$. So

$$\begin{aligned} \theta_u(x) &= \theta_v(x - v)/\theta_v(v - x) \\ &= \eta_W[l[v], v - x + \vartheta](x - v + \vartheta) \end{aligned} \tag{6}$$

provided that $x \notin \mathcal{W} \cup \mathcal{W}_v$. Thanks to Equation (6), evaluating a canonical Theta function $\theta_u(x)$ reduces to the evaluation of one Eta functions. This can be done as explained in Section 2.4.

Proposition 4 (Evaluating canonical Theta functions)**.** *There exists a deterministic algorithm that takes as input a finite field* $\mathbf{K}$ *with cardinality* q*, a curve* C *of genus* $g \geq 1$ *over* $\mathbf{K}$*, a Theta characteristic* Θ *defined over* $\mathbf{K}$*, an odd prime integer* $l \neq p$*, and two points* u *and* x *in* $J_C(\mathbf{K})$ *such that* $lu = 0$*, and*

$$x \notin \mathcal{W} \cup \mathcal{W}_v,$$

where

$$v = \frac{l+1}{2} \times u \in J_C(\mathbf{K}).$$

The algorithm computes $\theta_u(x)$ *in time* $(gl)^{\mathfrak{O}} \times (\log q)^{1+\mathfrak{e}(q)}$.

According to Remark 1 we can accelerate the computation using fast exponentiation. The resulting algorithm will fail when the argument x belongs to the support of the divisor of some intermediate factor.

Proposition 5 (Fast evaluation of canonical Theta functions)**.** *There exists a deterministic algorithm that takes as input a finite field* $\mathbf{K}$ *with cardinality* q*, a curve* C *of genus* $g \geq 1$ *over* $\mathbf{K}$*, a Theta characteristic* Θ *defined over* $\mathbf{K}$*, an odd prime integer* $l \neq p$*, and two points* u *and* x *in* $J_C(\mathbf{K})$ *such that* $lu = 0$*. The algorithm computes* $\theta_u(x)$ *in time* $g^{\mathfrak{O}} \times (\log q)^{1+\mathfrak{e}(q)} \times \log l$*. The algorithm may fail, in which case it returns no answer. For each* u*, the proportion of* x *in* $J_C(\mathbf{K})$ *for which the algorithm fails is* $\leq g^{\mathfrak{O}g} \times \log(l)/q$.

5. Quotients of Jacobians

Let $V \subset J_C[l]$ be a maximal isotropic subgroup for the commutator pairing, let $A = J_C/V$, and let $f : J_C \to A$ be the quotient map. Let $L = \mathcal{O}_{J_C}(l\mathcal{W})$. The map $v \mapsto \mathbf{a}_v$ is a homomorphism $V \to \mathcal{G}(L)$ lifting the inclusion $V \subset J_C[l]$. This canonical lift provides a descent datum for L onto A. We call M the corresponding line bundle on J_C/V. This is a symmetric principal polarization. In particular $h^0(M) = 1$ and there is a unique effective divisor Y on A associated with M. We set $X = f^*Y$. This is an effective divisor linearly equivalent to $l\mathcal{W}$ and invariant by V. Let $\mathfrak{u} = \sum_{1 \leq i \leq I} e_i[u_i]$ be a zero-cycle in J_C. Let y be a point on J_C. We assume that y does not belong to the support of the divisor $\sum_{1 \leq i \leq I} e_i X_{u_i} - X_{s(\mathfrak{u})} - (\deg(\mathfrak{u}) - 1)X$. Call $\eta_X[\mathfrak{u}, y]$ the unique function on J_C having divisor

$$(\eta_X[\mathfrak{u}, y]) = \sum_{1 \leq i \leq I} e_i X_{u_i} - X_{s(\mathfrak{u})} - (\deg(\mathfrak{u}) - 1)X$$

and such that

$$\eta_X[\mathfrak{u}, y](y) = 1.$$

This definition is additive in the sense that

$$\eta_X[\mathfrak{u} + \mathfrak{v}, y] = \eta_X[\mathfrak{u}, y] \times \eta_X[\mathfrak{v}, y] \times \eta_X[[s(\mathfrak{u})] + [s(\mathfrak{v})], y]$$

whenever it makes sense. We write $\eta_X[\mathfrak{u}] \in \mathbf{K}(J_C)^*/\mathbf{K}^*$ when we consider an Eta function up to a multiplicative scalar. Set $v_i = f(u_i) \in J_C/V$ for every $1 \le i \le I$ and let $\mathfrak{v} = f(\mathfrak{u}) = \sum_{1\le i\le I} e_i[v_i]$ be the image of $\mathfrak{u}$ in $\mathcal{Z}_0(J_C/V)$. There is a function with divisor $\sum_{1\le i\le I} e_i Y_{v_i} - Y_{s(\mathfrak{v})} - (\deg(\mathfrak{v}) - 1)Y$ on J_C/V. Composing this function with f we obtain a function on J_C having the same divisor as $\eta_X[\mathfrak{u}, y]$. So $\eta_X[\mathfrak{u}, y]$ is invariant by V and can be identified with the unique function on $A = J_C/V$ with divisor $\sum_{1\le i\le I} e_i Y_{v_i} - Y_{s(\mathfrak{v})} - (\deg(\mathfrak{v}) - 1)Y$, and taking value 1 at $f(y)$. When dealing with the quotient $A = J_C/V$ it will be useful to represent a point z on A by a point x on J_C such that $f(x) = z$. Such an x is in turn represented by a divisor $D_x - gO$ on C. It is then natural to evaluate functions like $\eta_X[\mathfrak{u}, y]$ at such an x. For example, taking $\mathfrak{u} = l[u]$ for u an m-torsion point, the function $\eta_X[\mathfrak{u}, y]$ is essentially a Theta function of level m for the quotient J_C/V. Evaluating such functions at a few points, we find projective equations for A. This will show very useful in Section 6. Section 5.1 provides an expression of $\eta_X[\mathfrak{u}, y]$ as a product involving a function Φ_V defined as an eigenvalue for the canonical lift of V in $\mathcal{G}(L)$. The complexity of evaluating Φ_V is bounded in Section 5.2.

5.1. **Explicit descent.** We need a function with divisor $X - l\mathcal{W}$ on J_C. Let $V^D = \mathrm{Hom}(V, \mathbf{G}_m)$ be the dual of V. For every character χ in V^D we denote H_χ the 1-dimensional subspace of $H^0(J_C, \mathcal{O}_{J_C}(l\mathcal{W}))$ where V acts through multiplication by χ. Then

$$\mathbf{a}_V = \sum_{v\in V} \mathbf{a}_v$$

is a surjection from $H^0(J_C, \mathcal{O}(l\mathcal{W}))$ onto H_1. We pick a random function in $H^0(J_C, \mathcal{O}(l\mathcal{W}))$ as explained in Proposition 1, and apply $\mathbf{a}_V$ to it. With probability $\ge 1/2$ the resulting function is a non-zero function in H_1. We call Φ_V this function. We shall explain in Section 5.2 how to evaluate Φ_V at a given point on J_C. We now explain how to express any $\eta_X[\mathfrak{u}]$ as a multiplicative combination of Φ_V and its translates. Without loss of generality we can assume that $s(\mathfrak{u}) = 0$ and $\deg(\mathfrak{u}) = 0$. We assume that $y \notin \bigcup_i \mathcal{W}_{u_i} \cup \bigcup_i X_{u_i}$. The composition $\Phi_V \circ t_{-u_i}$ has divisor $X_{u_i} - l\mathcal{W}_{u_i}$. The composition $\eta_W[\mathfrak{u}, y + \vartheta] \circ t_\vartheta$ has divisor $\sum_i e_i \mathcal{W}_{u_i}$. So

$$\eta_X[\mathfrak{u}, y](x) = (\eta_W[\mathfrak{u}, y + \vartheta](x + \vartheta))^l \times \prod_{1\le i\le I} (\Phi_V(x - u_i))^{e_i} \times \prod_{1\le i\le I} (\Phi_V(y - u_i))^{-e_i}.$$

5.2. **Evaluating functions on J_C/V.**

We now bound the cost of evaluation Φ_V at a given point $x \in J_C$. We assume that l is odd and prime to the characteristic p of $\mathbf{K}$. We are given two integers a and b such that $a + b = l$, and two elements u and y in $J_C(\mathbf{K})$ such that $y \notin \mathcal{W} \cup \mathcal{W}_{au} \cup \mathcal{W}_{-bu}$. The function Φ_V is the image by $\mathbf{a}_V$ of some function τ in $H^0(J_C, \mathcal{O}_{J_C}(l\mathcal{W}))$. We choose τ to be the function $\tau[u, y + \vartheta] \circ t_\vartheta = \eta_W[b[au] + a[-bu], y + \vartheta] \circ t_\vartheta$. The $\mathbf{K}$-scheme V is given by a collection of field extensions $(\mathbf{L}_i/\mathbf{K})_{1\le i\le I}$ and a point $w_i \in V(\mathbf{L}_i)$ for every i such that V is the disjoint union of the $\mathbf{K}$-Zariski closures of all w_i. In particular $\sum_i d_i = l^g$ where d_i is the degree of $\mathbf{L}_i/\mathbf{K}$ and the $\mathbf{L}_i$ are the minimum fields of definition for the w_i. Equivalently we may be given a separable algebra $\mathbf{L} = \mathbf{K}[V]$ of degree l^g over $\mathbf{K}$ and a point $\boldsymbol{w}$ in $V(\mathbf{L}) \subset J_C(\mathbf{L})$. We are given an element x in $J_C(\mathbf{K})$ such that $x \notin \mathcal{W} + V$. The value

$$\mathbf{a}_{\boldsymbol{w}}(\tau)(x) = \theta_{\boldsymbol{w}}(x) \times \tau(x - \boldsymbol{w}) = \theta_{\boldsymbol{w}}(x) \times \eta_W[b[au] + a[-bu], y + \vartheta](x - \boldsymbol{w} + \vartheta)$$

of $\mathbf{a}_{\boldsymbol{w}}(\tau)$ at x is an element of the affine algebra $\mathbf{K}[V]$. Its trace over $\mathbf{K}$ is equal to $\Phi_V(x)$.

Theorem 2 (Evaluating functions on quotients J_C/V)**.** *There exists a deterministic algorithm that takes as input a finite field $\mathbf{K}$ with characteristic p and cardinality q, a curve C of genus $g \geq 2$ over $\mathbf{K}$, a zero-cycle $\mathfrak{u} = \sum_{1\leq i\leq I} e_i[u_i]$ on the Jacobian J_C of C, a Theta characteristic Θ defined over $\mathbf{K}$, an odd prime integer $l \neq p$, a maximal isotropic $\mathbf{K}$-subgroup scheme $V \subset J_C[l]$, two classes x and y in $J_C(\mathbf{K})$ such that $y \notin \bigcup_i \mathcal{W}_{u_i} \cup \bigcup_i X_{u_i}$. The algorithm computes $\eta_X[\mathfrak{u}, y](x)$ in time $I \times \log|e| \times g^{\mathfrak{O}} \times (\log q)^{1+\mathfrak{e}(q)} \times l^{g(1+\mathfrak{e}(l^g))}$, where $|e| = \sum_{1\leq i\leq I}|e_i|$ is the ℓ^1-norm of e. The algorithm may fail, in which case it returns no answer. For each triple $(V, \mathfrak{u}, y)$, the proportion of x in $J_C(\mathbf{K})$ for which the algorithm fails is $\leq I \times \log|e| \times g^{\mathfrak{O}g} \times l^{g^2} \times \log l/q$.*

6. Curves of genus two

In this section we assume that the characteristic p of $\mathbf{K}$ is odd. We bound the complexity of computing an isogeny $J_C \to J_D$ between two Jacobians of dimension two. We give in Section 6.1 the expected form of such an isogeny. We give a differential characterization of it in Section 6.2. As a consequence of these differential equations we can compute such an isogeny in two steps: we first compute the image of a $(\mathbf{K}[t]/t^3)$-point on C by the isogeny, then lift to $\mathbf{K}[[t]]$. We explain in Section 6.3 how to compute images of points. This finishes the proof of Theorem 3 below.

6.1. **Algebraic form.** Let C be a curve of genus 2 over $\mathbf{K}$. We assume that C is given by the affine singular model

$$v^2 = h_C(u) \tag{7}$$

where h_C is a polynomial of degree 5. Let O_C be the unique place at infinity. Let J_C be the Jacobian of C and let $j_C : C \to J_C$ be the Jacobi map with origin O_C. Let D be another curve of genus 2 over $\mathbf{K}$. We assume that D is given by the affine singular model $y^2 = h_D(x)$ where h_D is a polynomial of degree 5 or 6. Let K_D be a canonical divisor on D. Call $D^{(2)}$ the symmetric square of D and let $j_D^{(2)} : D^{(2)} \to J_D$ be the map sending the pair $\{Q_1, Q_2\}$ onto the class $z = j_D^{(2)}(\{Q_1, Q_2\})$ of $Q_1 + Q_2 - K_D$. This is a birational morphism. We define the Mumford coordinates

$$\begin{aligned}
\mathbf{s}(z) &= x(Q_1) + x(Q_2),\\
\mathbf{p}(z) &= x(Q_1) \times x(Q_2),\\
\mathbf{q}(z) &= y(Q_1) \times y(Q_2),\\
\mathbf{r}(z) &= (y(Q_2) - y(Q_1))/(x(Q_2) - x(Q_1)).
\end{aligned}$$

The function field of J_D is $\mathbf{K}(\mathbf{s}, \mathbf{p}, \mathbf{q}, \mathbf{r})$. The function field of the Kummer variety of D is $\mathbf{K}(\mathbf{s}, \mathbf{p}, \mathbf{q})$. We assume that there exists an isogeny $f : J_C \to J_D$ with kernel V, a maximal isotropic group in $J_C[l]$, where l is an odd prime different from the characteristic p of $\mathbf{K}$. We define $F : C \to J_D$ to be the composite map $f \circ j_C$. The exists a unique morphism $G : C \to D^{(2)}$ such that the following diagram commutes.

$$\begin{tikzcd} & D^{(2)} \arrow[dd, "j_D^{(2)}"] \\ C \arrow[ur, "G"] \arrow[dr, "F"'] & \\ & J_D. \end{tikzcd}$$

For every point $P = (u, v)$ on C we have $F((u, -v)) = -F(P)$. We deduce the following algebraic description of the map F

$$\begin{aligned} \mathbf{s}(F(P)) &= \mathbf{S}(u), \\ \mathbf{p}(F(P)) &= \mathbf{P}(u), \\ \mathbf{q}(F(P)) &= \mathbf{Q}(u), \\ \mathbf{r}(F(P)) &= v\mathbf{R}(u), \end{aligned} \tag{8}$$

where $\mathbf{S}$, $\mathbf{P}$, $\mathbf{Q}$, $\mathbf{R}$ are rational fractions in one variable. Let O_D be a point on D. Let Z be the algebraic subset of $D^{(2)}$ consisting of pairs $\{O_D, Q\}$ for some Q in D. Let $T \subset J_D$ be the image of Z by $j_D^{(2)}$. This is a divisor with self intersection

$$T.T = 2.$$

The image $F(C)$ of C by F is algebraically equivalent to lT. The divisors of poles of the functions $\mathbf{s}$, $\mathbf{p}$, $\mathbf{q}$, and $\mathbf{r}$, are algebraically equivalent to $2T$, $2T$, $6T$, and $4T$, respectively. Seen as functions on C, the functions $\mathbf{S}(u)$, $\mathbf{P}(u)$, $\mathbf{Q}(u)$, and $v\mathbf{R}(u)$, thus have degrees bounded by $4l$, $4l$, $12l$, and $8l$, respectively. So the rational fractions $\mathbf{S}$, $\mathbf{P}$, $\mathbf{Q}$, and $\mathbf{R}$, have degrees bounded by $2l$, $2l$, $6l$, and $4l + 3$, respectively. The four rational fractions $\mathbf{S}$, $\mathbf{P}$, $\mathbf{Q}$, $\mathbf{R}$ provide a compact description of the isogeny f from which we can deduce any desirable information about it.

6.2. **Differential system.** The morphism $F : C \to J_D$ induces a map

$$F^* : H^0(\Omega^1_{J_D/\mathbf{K}}) \to H^0(\Omega^1_{C/\mathbf{K}}).$$

A consequence of this is that the vector $(\mathbf{S}, \mathbf{P}, \mathbf{Q}, \mathbf{R})$ satisfies a first order differential system. This system can be given a convenient form using local coordinates. A basis for $H^0(\Omega^1_{C/\mathbf{K}})$ is made of du/v and udu/v. We identify $H^0(\Omega^1_{J_D/\mathbf{K}})$ with the invariant subspace of $H^0(\Omega^1_{D\times D/\mathbf{K}})$ by the permutation of the two factors. We deduce that a basis for this space is made of $dx_1/y_1 + dx_2/y_2$ and $x_1dx_1/y_1 + x_2dx_2/y_2$. Let $M = (m_{i,j})_{1\le i,j\le 2}$ be the matrix of F^* with respect to these two bases. So

$$\begin{aligned} F^*(dx_1/y_1 + dx_2/y_2) &= (m_{1,1} + m_{2,1} \times u) \times du/v, \\ F^*(x_1dx_1/y_1 + x_2dx_2/y_2) &= (m_{1,2} + m_{2,2} \times u) \times du/v. \end{aligned} \tag{9}$$

Let $P = (u_P, v_P)$ be a point on C. We assume that $v_P \neq 0$. Let Q_1 and Q_2 be two points on D such that $F(P)$ is the class of $Q_1 + Q_2 - K_D$. We assume that $F(P) \neq 0$, so the divisor $Q_1 + Q_2$ is non-special. We also assume that $Q_1 \neq Q_2$ and either of the points are defined over $\mathbf{K}$. Let t be a formal parameter. Set $\mathbf{L} = \mathbf{K}((t))$. We call

$$P(t) = (u(t), v(t))$$

the point on $C(\mathbf{L})$ corresponding to the value t of the local parameter $u - u_P$ at P. The image of $P(t)$ by F is the class of $Q_1(t) + Q_2(t) - K_D$ where $Q_1(t)$ and $Q_2(t)$ are two $\mathbf{L}$-points on D.

$$\begin{tikzcd} \operatorname{Spec}\mathbf{K}[[t]] \arrow[rr, "t\mapsto(Q_1(t),Q_2(t))"] \arrow[d, "t\mapsto P(t)"] & & D \times D \arrow[d] \\ C \arrow[rr, "F"] & & J_D. \end{tikzcd} \tag{10}$$

From Equations (9) and the commutativity of diagram (10) we deduce that the coordinates $(x_1(t), y_1(t))$ and $(x_2(t), y_2(t))$ of $Q_1(t)$ and $Q_2(t)$ satisfy the following non-singular first order system of differential equations.

$$\left\{ \begin{array}{ccc} \frac{\dot{x}_1(t)}{y_1(t)} + \frac{\dot{x}_2(t)}{y_2(t)} & = & \frac{(m_{1,1}+m_{2,1}\times u(t))\times \dot{u}(t)}{v(t)}, \\ \frac{x_1(t)\times\dot{x}_1(t)}{y_1(t)} + \frac{x_2(t)\times\dot{x}_2(t)}{y_2(t)} & = & \frac{(m_{1,2}+m_{2,2}\times u(t))\times \dot{u}(t)}{v(t)}, \\ y_1(t)^2 & = & h_D(x_1(t)), \\ y_2(t)^2 & = & h_D(x_2(t)). \end{array} \right. \tag{11}$$

So we can recover the complete description of the isogeny, namely the rational fractions $\mathbf{S}$, $\mathbf{P}$, $\mathbf{Q}$, $\mathbf{R}$, from the knowledge of the image by F of a *single* formal point on C. More concretely, we compute the image $\{Q_1(t), Q_2(t)\}$ of $P(t)$ by G with low accuracy, then deduce from Equation (11) the values of the four scalars $m_{1,1}$, $m_{1,2}$, $m_{2,1}$, $m_{2,2}$. Then use Equation (11) again to increase the accuracy of the formal expansions up to $O(t^{\mathfrak{O}l})$ and recover the rational fractions from their expansions using continued fractions. Coefficients of $x_1(t)$ and $x_2(t)$ can be computed one by one using Equation (11). Reaching accuracy $\mathfrak{O}l$ then requires $\mathfrak{O}l^2$ operations in $\mathbf{K}$. We can also use more advanced methods [4, 3] with quasi-linear complexity in the expected accuracy of the result. Both methods may produce zero denominators if the characteristic is small. In that case we use a trick introduced by Joux and Lercier [13] in the context of elliptic curves. We lift to a p-adic field having $\mathbf{K}$ as residue field. The denominators introduced by (11) do not exceed $p^{\mathfrak{O}\log(l)}$. The required p-adic accuracy, and the impact on the complexity are thus negligible.

6.3. **Computing isogenies.** Given a curve C of genus two and a maximal isotropic subspace V in $J_C[l]$ we set $A = J_C/V$ and call Y the polarization introduced in Section 5. We use the methods given in Sections 3 and 5 to find nine functions $\eta_0 = 1, \eta_1, \ldots, \eta_8$, such that $(\eta_0, \eta_1, \eta_2, \eta_3)$ is a basis of $H^0(A, \mathcal{O}_A(2Y))$ and $(\eta_0, \ldots, \eta_8)$ is a basis of $H^0(A, \mathcal{O}_A(3Y))$. We thus define two maps $e_2 : A \to \mathbf{P}^3$ and $e_3 : A \to \mathbf{P}^8$. Denoting $\pi : \mathbf{P}^8 \dashrightarrow \mathbf{P}^3$ the projection

$$\pi(Z_0 : Z_1 : \cdots : Z_8) = (Z_0 : Z_1 : Z_2 : Z_3)$$

we have $\pi \circ e_3 = e_2$. Evaluating the $(\eta_i)_{0\le i\le 8}$ at enough points we find equations for $e_3(A)$ and $e_2(A)$. The intersection of $e_3(A)$ with the hyperplane H_0 with equation $Z_0 = 0$ in $\mathbf{P}^8$ is $e_3(Y)$ counted with multiplicity 3. We now assume that Y is a smooth and absolutely integral curve of genus two. This is the generic case, and it is true in particular whenever the Jacobian J_C of C is absolutely simple. The intersection of $e_2(A)$ with the hyperplane with equation $Z_0 = 0$ in $\mathbf{P}^3$ is $e_2(Y)$ counted with multiplicity 2. The map $Y \to e_2(Y)$ has degree two. Its image $e_2(Y)$ is a plane curve of degree two. The map $Y \to e_2(Y)$ is the hyperelliptic quotient. We deduce explicit equations for a hyperelliptic curve D and an isomorphism $D \to Y$.

We now define a rational map φ from J_C into the symmetric square of $D \simeq Y$ by setting, for z a generic point on J_C,

$$\varphi(z) = Y_{f(z)} \cap Y, \tag{12}$$

where $Y_{f(z)}$ is the translate of Y by $f(z)$. Let O_C be a Weierstrass point on C. We define a map ψ from C into the symmetric square of $D \simeq Y$ by setting, for $P \in C$ un generic point, $\psi(P) = \varphi(P - O_C)$. We check that $\psi(O_C)$ is a canonical divisor K_Y on Y. The difference $\psi(P) - \psi(O_C)$ is a degree 0 divisor on Y and belongs to the class $f(P - O_C)$. So $\psi : C \to Y^{(2)}$ is the map G introduced in Section 6.1. We explain how to evaluate the map φ at a given z in J_C. The main point is to compute the intersection in Equation (12). This is a matter of linear algebra. We pick two auxiliary classes z_1 and z_2 in J_C. We set $z_1' = -z - z_1$ and $z_2' = -z - z_2$. We assume that $\varphi(z_1)$, $\varphi(z_2)$, $\varphi(z_1')$, $\varphi(z_2')$ are pairwise disjoint. Seen as a function on $A = J_C/V$, the function $\eta_X[[z_1] + [z_1'] + [z]]$ belongs to $H^0(A, \mathcal{O}_A(3Y))$. Evaluating it at a few points we can express it as a linear combination of the elements $(\eta_i)_{0\le i\le 8}$ of our basis:

$$\eta_X[[z_1] + [z_1'] + [z]] = \sum_{0\le i\le 8} c_i \times \eta_i.$$

The hyperplane section H_1 with equation $\sum_i c_i Z_i = 0$ intersects $e_3(A)$ at $Y_{f(z_1)} + Y_{f(z_1')} + Y_{f(z)}$. We similarly find an hyperplane section H_2 with equation $\sum_i d_i Z_i = 0$ intersecting $e_3(A)$ at $Y_{f(z_2)} + Y_{f(z_2')} + Y_{f(z)}$. So

$$\varphi(z) = Y_{f(z)} \cap Y = H_1 \cap H_2 \cap H_0 \cap e_3(A),$$

is computed by linear substitutions. Altogether we have proven the theorem bellow.

Theorem 3 (Computing isogenies for genus two curves)**.** *There exists a probabilistic (Las Vegas) algorithm that takes as input a finite field $\mathbf{K}$ of odd characteristic p, an odd prime l different from p, a genus two curve C as in Equation (7), and a maximal isotropic subgroup V in $J_C[l]$ as in Section 5.2, such that the curve Y introduced in Section 5 is smooth and absolutely integral. The algorithm returns a genus two curve D and a map $F : C \to J_D$ as in Equation (8). The running time is $l^{2+\mathfrak{e}(l)} \times (\log q)^{1+\mathfrak{e}(q)}$.*

In case Y is not smooth and absolutely integral, it is a stable curve of genus two. The calculation above will work just as well and produce one map from C onto either of the components of Y. We do not formalize this degenerate case.

7. AN EXAMPLE

Let $\mathbf{K}$ be a field with 1009 elements. Let

$$h_C(u) = u(u-1)(u-2)(u-3)(u-85) \in \mathbf{K}[u]$$

and let C be the genus two curve given by the singular plane model with equation $v^2 = h_C(u)$. Let O_C be the place at infinity. Let T_1 be the effective divisor of degree 2 defined by the ideal

$$(u^2 + 247u + 67, v - 599 - 261u) \subset \mathbf{K}[u,v]/(v^2 - h_C(u)).$$

Let T_2 be the effective divisor of degree 2 defined by the ideal

$$(u^2 + 903u + 350, v - 692 - 98u) \subset \mathbf{K}[u,v]/(v^2 - h_C(u)).$$

The classes of $T_1 - 2O_C$ and $T_2 - 2O_C$ generate a totally isotropic subspace V of dimension 2 inside $J_C[3]$. Let $A = J_C/V$. Let $W \subset J_C$ be the set of classes of divisors $P - O_C$ for P a point on C. Since O_C is a Weierstrass point, we have $[-1]^*W = W$. Let $X \subset J_C$ and $Y \subset A$ be the two divisors introduced at the beginning of Section 5. Let $B \subset C$ be the effective divisor of degree 2 defined by the ideal $(u^2 + 862u + 49, v - 294 - 602u)$. Let $b \in J_C$ be the class of $B - 2O_C$. For i in $\{0,1,2,3,85\}$ let P_i be the point on C with coordinates $u = i$ and $v = 0$. The class of $P_i - O_C$ in J_C is also denoted P_i. We set $P_\infty = O_C$ and $P_+ = P_0 + P_1 \in J_C$.

For i in $\{\infty, 0, 1, +, 2, 3, 85\}$ let η_i be the unique function on J_C with divisor $2(X_{P_i} - X)$ and taking value 1 at b. These functions are invariant by V and may be seen as level two Theta functions on A. Evaluating these functions at a few points we check that $(\eta_\infty, \eta_0, \eta_1, \eta_+)$ form a basis of $H^0(A, \mathcal{O}_A(2Y))$ and

$$\begin{aligned}
\eta_2 &= 437\eta_\infty + 241\eta_0 + 332\eta_1,\\
\eta_3 &= 294\eta_\infty + 246\eta_0 + 470\eta_1,\\
\eta_{85} &= 639\eta_\infty + 827\eta_0 + 553\eta_1.
\end{aligned}$$

Call Z_∞, Z_0, Z_1, Z_+ the projective coordinates associated with $(\eta_\infty, \eta_0, \eta_1, \eta_+)$. The Kummer surface of A is defined by the vanishing of the following homogeneous form of degree four

$$\begin{aligned}
&597Z_\infty^2Z_0^2 + 14Z_\infty^2Z_0Z_1 + 781Z_\infty^2Z_0Z_+ + 819Z_\infty^2Z_1Z_+ + 835Z_\infty^2Z_1^2 + 615Z_\infty^2Z_+^2\\
&+401Z_\infty Z_0^2Z_1 + 833Z_\infty Z_0^2Z_+ + 553Z_\infty Z_0Z_1Z_+ + 843Z_\infty Z_0Z_1^2 + 206Z_\infty Z_0Z_+^2 + 418Z_\infty Z_1^2Z_+\\
&+321Z_\infty Z_1Z_+^2 + 796Z_0^2Z_1Z_+ + Z_0^2Z_1^2 + 1000Z_0^2Z_+^2 + 856Z_0Z_1^2Z_+ + 655Z_0Z_1Z_+^2 + 555Z_1^2Z_+^2.
\end{aligned}$$

This equation is found by evaluating all four functions at forty points. We set $Z_\infty = 0$ in this form and find the square of the following quadratic form

$$611Z_0Z_+ + 581Z_1Z_+ - Z_0Z_1 \tag{13}$$

which is an equation for $e_2(Y)$ in the projective plane $Z_\infty = 0$. Recall $e_2 : A \to \mathbf{P}^3$ is the map introduced in Section 6.3. Set

$$\begin{aligned}
Z_2 &= 437Z_\infty + 241Z_0 + 332Z_1\\
Z_3 &= 294Z_\infty + 246Z_0 + 470Z_1\\
Z_{85} &= 639Z_\infty + 827Z_0 + 553Z_1.
\end{aligned}$$

We find an affine parameterization of the conic $e_2(Y)$ in Equation (13) by setting

$$Z_+ = 1 \text{ and } Z_1 = xZ_0.$$

For i in $\{0, 1, +, 2, 3, 85\}$ call D_i the line with equations $\{Z_\infty = 0, Z_i = 0\}$. There are six intersection points between $e_2(Y)$ and one of the D_i. These are the six branched points of the hyperelliptic cover $Y \to e_2(Y)$. They correspond to the values

$$\{0, \infty, 513, 51, 243, 987\}$$

of the x parameter. We set

$$h_D(x) = x(x-513)(x-51)(x-243)(x-987) \in \mathbf{K}[x]$$

and let D be the genus two curve given by the singular plane model with equation $y^2 = h_D(x)$. Let O_D be the unique place at infinity on D. Let $P = (u, v)$ be a point on C. Using notation introduced in Section 6.1 we call $F(P)$ the image of $P - O_C$ in J_D and $G(P)$ an effective divisor such that $F(P) = G(P) - 2O_D$. This divisor is defined by the ideal

$$(x^2 - \mathbf{S}(u)x + \mathbf{P}(u), y - v(\mathbf{T}(u) + x\mathbf{R}(u)) \subset \mathbf{K}(u, v)[x, y]/(y^2 - h_D(x))$$

where

$$\begin{aligned}
\mathbf{S}(u) &= 354\frac{u^5 + 647u^4 + 931u^3 + 597u^2 + 73u + 361}{u^5 + 832u^4 + 811u^3 + 215u^2 + 420u},\\
\mathbf{P}(u) &= 50\frac{u^5 + 262u^4 + 812u^3 + 770u^2 + 868u + 314}{u^5 + 832u^4 + 811u^3 + 215u^2 + 420u},\\
\mathbf{R}(u) &= 304\frac{u^6 + 437u^5 + 623u^4 + 64u^3 + 194u^2 + 3u + 511}{u^8 + 239u^7 + 983u^6 + 800u^5 + 214u^4 + 489u^3 + 191u^2},\\
\mathbf{T}(u) &= 678\frac{u^6 + 697u^5 + 263u^4 + 895u^3 + 859u^2 + 204u + 130}{u^8 + 239u^7 + 983u^6 + 800u^5 + 214u^4 + 489u^3 + 191u^2}.
\end{aligned}$$

We note that the fraction $\mathbf{Q}(u)$ introduced in Section 6.1 is

$$\mathbf{Q} = h_C \times (\mathbf{T}^2 + \mathbf{R}^2 \times \mathbf{P} + \mathbf{S} \times \mathbf{R} \times \mathbf{T}).$$

We now explain how these rational fractions were computed. We consider the formal point

$$P(t) = (u(t), v(t)) = (832 + t, 361 + 10t + 14t^2 + O(t^3)) \in C.$$

We compute $G(P(t)) = \{Q_1(t), Q_2(t)\}$ and find

$$\begin{aligned}
Q_1(t) &= (x_1(t), y_1(t)) = (973 + 889t + 57t^2 + O(t^3), 45 + 209t + 39t^2 + O(t^3)),\\
Q_2(t) &= (x_2(t), y_2(t)) = (946 + 897t + 252t^2 + O(t^3), 911 + 973t + 734t^2 + O(t^3)).
\end{aligned}$$

Using Equation (11) we deduce the values

$$m_{1,1} = 186, m_{1,2} = 864, m_{2,1} = 853, m_{2,2} = 640.$$

Using Equation (11) again we increase the accuracy in the expansions for $x_1(t)$, $x_2(t)$, $y_1(t)$, and $y_2(t)$ then deduce the rational fractions $\mathbf{S}$, $\mathbf{P}$, $\mathbf{R}$, and $\mathbf{T}$.

REFERENCES

[1] H F Baker. *Abel's theorem and the allied theory, including the theory of the theta functions*. Cambridge Univ. Press, Cambridge, 1897.

[2] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2004.

[3] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77(263):1755–1778, 2008.

[4] R. P. Brent and H. T. Kung. Fast algorithms for manipulating formal power series. *J. Assoc. Comput. Mach.*, 25(4):581–595, 1978.

[5] Romain Cosset and Damien Robert. Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves. to appear in Mathematics of Computations, October 2013.

[6] Jean-Marc Couveignes. Computing V_f modulo p. In *Computational aspects of modular forms and Galois representations*, volume 176 of *Ann. of Math. Stud.*, pages 337–370. Princeton Univ. Press, Princeton, NJ, 2011.

[7] Jean-Marc Couveignes and Bas Edixhoven. First description of the algorithms. In *Computational aspects of modular forms and Galois representations*, volume 176 of *Ann. of Math. Stud.*, pages 69–78. Princeton Univ. Press, Princeton, NJ, 2011.

[8] Claus Diem. *On arithmetic and the discrete logarithm problem in class groups of curves*. Habilitation thesis. Leipzig, 2008.

[9] I. Dolgachev and D. Lehavi. On isogenous principally polarized abelian surfaces. In *Curves and abelian varieties*, volume 465 of *Contemp. Math.*, pages 51–69. Amer. Math. Soc., Providence, RI, 2008.

[10] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[11] John D. Fay. *Theta Functions on Riemann Surfaces*. Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, Vol. 352.

[12] Sudhir R. Ghorpade and Gilles Lachaud. Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Mosc. Math. J.*, 2(3):589–631, 2002. Dedicated to Yuri I. Manin on the occasion of his 65th birthday.

[13] Antoine Joux and Reynald Lercier. Counting points on elliptic curves in medium characteristic. Cryptology ePrint Archive, Report 2006/176, 2006.

[14] Kamal Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239, 2007.

[15] Gilles Lachaud and Mireille Martin-Deschamps. Nombre de points des jacobiennes sur un corps fini. *Acta Arith.*, 56(4):329–340, 1990.

[16] R. Lercier and F. Morain. Algorithms for computing isogenies between elliptic curves. In D.A. Buell and J.T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 77–96, Providence, 1998. American Mathematical Society & Internationnal Press. Held in 1995 at the University of Illinois at Chicago.

[17] David Lubicz and Damien Robert. Computing isogenies between abelian varieties. *Compos. Math.*, 148(5):1483–1515, 2012.

[18] David Lubicz and Damien Robert. Computing separable isogenies in quasi-optimal time. February 2014.

[19] Nicolas Mascot. Computing modular Galois representations. *Rend. Circ. Mat. Palermo (2)*, 62(3):451–476, 2013.

[20] Victor S. Miller. The Weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.

[21] David Mumford. *Tata lectures on theta. III*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. With collaboration of Madhav Nori and Peter Norman, Reprint of the 1991 original.

[22] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[23] Bjorn Poonen. Computational aspects of curves of genus at least 2. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 283–306. Springer, Berlin, 1996.

[24] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[25] N. Shepherd-Barron. Thomae's formulae for non-hyperelliptic curves and spinorial square roots of theta-constants on the moduli space of curves. *ArXiv e-prints*, February 2008.

[26] Benjamin Smith. Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 159–170. Amer. Math. Soc., Providence, RI, 2012.

[27] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[28] Jacques Vélu. Courbes elliptiques munies d'un sous-groupe $\mathbf{Z}/n\mathbf{Z}\times\mu_n$. *Bull. Soc. Math. France Mém.*, (57):5–152, 1978.

[29] Emil J. Volcheck. Computing in the Jacobian of a plane algebraic curve. In *Algorithmic number theory (Ithaca, NY, 1994)*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 221–233. Springer, Berlin, 1994.

[30] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041, Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[31] André Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064, Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, CNRS, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, INRIA, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, LABORATOIRE INTERNATIONAL DE RECHERCHE EN INFORMATIQUE ET MATHÉMATIQUES APPLIQUÉES

E-mail address: `Jean-Marc.Couveignes@u-bordeaux.fr`

TONY EZOME, UNIVERSITÉ DES SCIENCES ET TECHNIQUES DE MASUKU, FACULTÉ DES SCIENCES, DÉPARTEMENT DE MATHÉMATIQUES ET INFORMATIQUE, BP 943 FRANCEVILLE, GABON.

TONY EZOME, LABORATOIRE INTERNATIONAL DE RECHERCHE EN INFORMATIQUE ET MATHÉMATIQUES APPLIQUÉES

E-mail address: `latonyo2000@yahoo.fr`